

FIG. 1

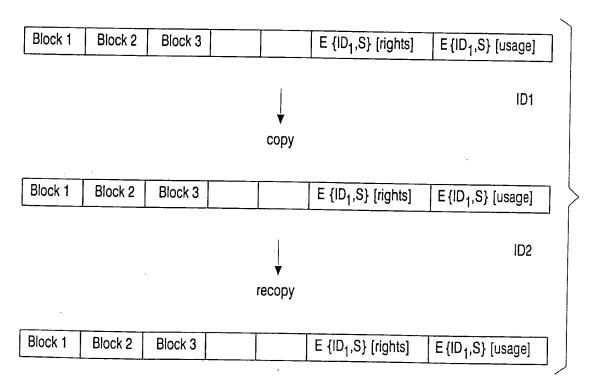
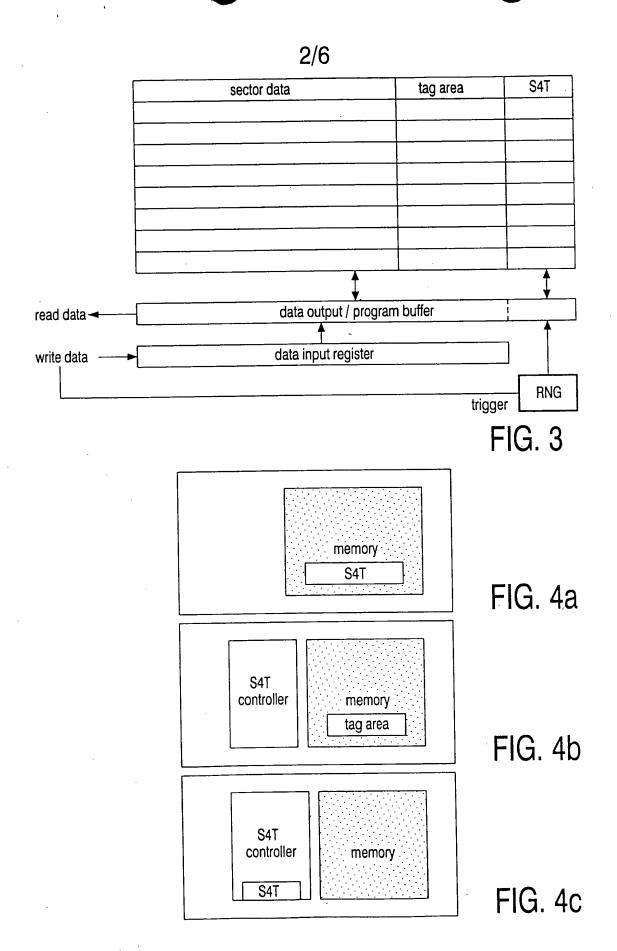
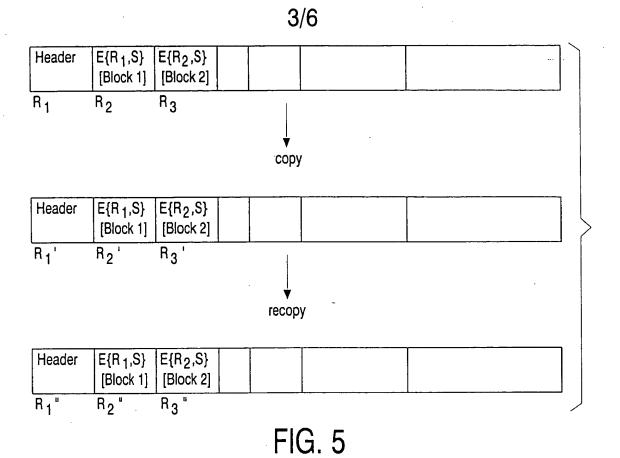


FIG. 2

ID1





sector data tag area 547 E<sub>k</sub> [content]  $R_1$ E<sub>k</sub>[content]  $R_2$ E<sub>k</sub>[content]  $R_3$  $R_{\mathsf{n}}$ E<sub>k</sub> [ content ]  $R_{n+1}$ rights info  $R_{n+2}$ usage info R<sub>n+3</sub>  $E_k,[K]$  $K' = H(R_1, ..., R_{n+2}, S)$ 

FIG. 6a

4/6

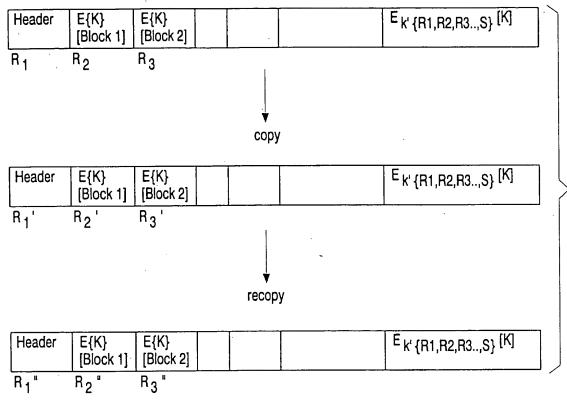


FIG. 6b

Sector data	S4T
$ID_A$ , Enc [K $_{Pub, A}$ ; S, $ID_A$ , x, y]	T <sub>1</sub>
IDA, Enc[K Priv, A; H[T <sub>1</sub> , S, ID <sub>A</sub> , x, y]]	T <sub>2</sub>
E [ K ; audio ]	TJ
•••	
E [ K; audio ]	TN
rights info	$T_{N+1}$
usage info	T <sub>N+2</sub>
Enc[H[T <sub>J</sub> ,,T <sub>N</sub> ,T <sub>N+1</sub> ,T <sub>N+2</sub> ,S];K]	

FIG. 7

## 5/6

Sector data	S4T
ID <sub>A</sub> , Enc[K <sub>Pub, A</sub> ; S, ID <sub>A</sub> , x, y]	T <sub>1</sub>
IDA, Enc[K <sub>Priv, A</sub> ; H[T <sub>1</sub> , S, ID <sub>A</sub> , x, y]]	T <sub>2</sub>
ID <sub>B</sub> , Cert (K <sub>Pub, B</sub> )	
E [ K ; audio ]	Tj
	• • •
E[K; audio]	TN
rights info	T <sub>N+1</sub>
usage info	T <sub>N+2</sub>
Enc [H [ $T_J$ ,, $T_N$ , $T_{N+1}$ , $T_{N+2}$ , S]; K]	•••

FIG. 8

Sector data	S4T
ID <sub>A</sub> , Enc[K <sub>Pub, A</sub> ; S, ID <sub>A</sub> , x, y]	T <sub>1</sub>
<pre>IDA, Enc[K Priv, A; H[T<sub>1</sub>, S, IDA, x, y]]</pre>	T <sub>2</sub>
IDB, Enc[K <sub>Pub, B</sub> , S, ID <sub>A</sub> , T <sub>1</sub> , T <sub>2</sub> ]	Тз
E [ K ; audio ]	TJ
E [ K ; audio ]	TN
rights info	T <sub>N+1</sub>
usage info	T <sub>N+2</sub>
Enc[H[T <sub>J</sub> ,,T <sub>N</sub> ,T <sub>N+1</sub> ,T <sub>N+2</sub> ,S];K]	

FIG. 9

## 6/6

Sector data	S4T
ID <sub>A</sub> , Enc[K <sub>Pub, A</sub> ; S, ID <sub>A</sub> , x, y]	Т1
ID <sub>A</sub> , Enc [ K <sub>Priv, A</sub> ; H [ T <sub>1</sub> , S, ID <sub>A</sub> , x, y ]]	T <sub>2</sub>
ID <sub>B</sub> , Enc[K <sub>Pub,B</sub> ; S,ID <sub>B</sub> ,p,q]	Тз
ID <sub>B</sub> , Enc [ K <sub>Priv, B</sub> ; H [ T <sub>3</sub> , S, ID <sub>B</sub> , p, q ]]	T <sub>4</sub>
E [ K ; audio ]	TJ
	• • •
E[K; audio]	T <sub>N</sub>
rights info	T <sub>N+1</sub>
usage info	T <sub>N+2</sub>
Enc[H[T <sub>J</sub> ,, T <sub>N</sub> , T <sub>N+1</sub> , T <sub>N+2</sub> , S]; K]	

FIG. 10

Sector data	S4T
ID <sub>A</sub> , Enc[K <sub>Pub, A</sub> ; S,ID <sub>A</sub> , x, y]	Τ <sub>1</sub>
$ID_A$ , Enc [K $_{Priv, LMC}$ ; H[T $_1$ , S, $ID_A$ , x, y]]	T <sub>2</sub>
IDB, Enc[K Pub, B; S, IDB, p, q]	T <sub>3</sub>
$ID_B$ , Enc [ K $_{Priv, LMC}$ ; H [ $T_3$ , S, $ID_B$ , $p$ , $q$ ]]	Τ <sub>4</sub>
ID <sub>LMC</sub> Cert (K <sub>Pub, LMC</sub> )	
E [ K ; audio ]	TJ
E [ K ; audio ]	TN
rights info	$T_{N+1}$
usage info	T <sub>N+2</sub>
Enc[H[ $T_J$ ,, $T_N$ , $T_{N+1}$ , $T_{N+2}$ , S]; K]	

FIG. 11